Claims

1. A method to delivery encrypted digital content from a first system for playing the content to a second system for playing the content, the method on a second system comprising the steps of:

reading on a second system from a computer readable medium metadata which has previously been associated, wherein in the content is encrypted with a first key associated with the first system;

selecting from the metadata associated content to decrypt;

establishing a secure transmission with an authorization authority for decrypting the content; and

receiving a decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted.

2. The method according to claim 1, further comprising the steps of:

playing at least part of the previously encrypted content by decrypting the encrypted content with the decrypting key.

3. The method according to claim 2, wherein the step of decrypting is performed in a tamper-resistant environment for deterring unauthorized access to the decrypting key.

4. The method according to claim 1, wherein the step of decrypting further comprises:

decrypting at least part of the previously encrypted content as permitted;

reencrypting the decrypted content utilizes a unique local decrypting key;

storing the content in a library; and

decrypting at least part of the content from the library using the unique local decrypting key

5. The method according to claim 4, wherein the steps of decrypting and reencrypting is performed in a tamper-resistance environment for deterring unauthorized access to the decrypting key.

6. A method to delivery encrypted digital content from a first end user system for playing the content to a second end user system for playing the content, the method on the first end user system comprising the steps of:

reading from a computer readable medium metadata which has previously been associated with the content;

selecting from the metadata associated content to decrypt;

establishing a secure connection with an authorization authority for decrypting the content;

receiving a secure container containing the decrypting key for decrypting at least part of the previously encrypted content as permitted;

creating an secure container using the encrypting key from a clearinghouse, wherein the secure container has an encrypting key therein from the first end user system;

transferring the secure container to the clearinghouse for authentication of permission to decrypt the content;

receiving from the clearinghouse, a secure container encrypted using the encrypting key of the first end user system containing the decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted; and

creating a container for distribution to a second end user system for playing the content which has been reencrypted with a new encrypting key associated with the first end user system.

7. The method according to claim 6, wherein the step of playing further comprises playing at least part of the previously encrypted content comprising a plurality of distinct titles whereby each distinct title is decrypted with a unique decrypting key.

8. The method according to claim 6, wherein the step of establishing a secure connecting further comprises the step of transmitting a credit information to the authorization authority.

9. The method according to claim 6, wherein the metadata is stored as part of a promotional package on a CD or DVD containing non-encrypted content.

10. A computer readable medium containing programming instructions for delivery of encrypted digital content from a first system for playing the content to a second system for playing the content, the programming instructions for execution on a second user system comprising:

reading on a second system from a computer readable medium metadata which has previously been associated, wherein in the content is encrypted with a first key associated with the first system;

selecting from the metadata associated content to decrypt;

establishing a secure transmission with an authorization authority for decrypting the content;

receiving a decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted.

11. The computer readable medium according to claim 10, wherein the programming instruction of decrypting is performed in a tamper-resistant environment for deterring unauthorized access to the decrypting key.

12. The computer readable medium according to claim 10, wherein the programming instruction of decrypting further comprises:

decrypting at least part of the previously encrypted content as permitted;

reencrypting the decrypted content utilizes a unique local decrypting key;

storing the content in a library; and

decrypting at least part of the content from the library using the unique local decrypting key.

13. The computer readable medium according to claim 12, wherein the programming instruction of decrypting and reencrypting is performed in a tamper-resistance environment for deterring unauthorized access to the decrypting key.

14. A computer readable medium containing programming instructions for delivering encrypted digital content from a first end user system for playing the content to a second end user system for playing the content, the programming instructions for execution on a first user system comprising:

reading from a computer readable medium metadata which has previously been associated with the content;

selecting from the metadata associated content to decrypt;

establishing a secure connection with an authorization authority for decrypting the content;

receiving a secure container containing the decrypting key for decrypting at least part of the previously encrypted content as permitted;

creating an secure container using the encrypting key from a clearinghouse, wherein the secure container has an encrypting key therein from the first end user system;

transferring the secure container to the clearinghouse for authentication of permission to decrypt the content;

receiving from the clearinghouse, a secure container encrypted using the encrypting key of the first end user system containing the decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted; and

creating a container for distribution to a second end user system for playing the content which has been reencrypted with a new encrypting key associated with the first end user system.

15. The computer readable medium according to claim 14, wherein the programming instruction of playing further comprises playing at least part of the previously encrypted content comprising a plurality of distinct titles whereby each distinct title is decrypted with a unique decrypting key.

16. The computer readable medium according to claim 14, wherein the programming instruction of establishing a secure connecting further comprises the step of transmitting a credit information to the authorization authority.

17. The computer readable medium according to claim 14, wherein the metadata is stored as part of a promotional package on a CD or DVD containing non-encrypted content.

18. A first end user system for delivery of encrypted digital content to a second end user system for playing the content, the first end user system comprising:

an interface for reading from a computer readable medium metadata which has previously been associated with the content;

an input device for receiving at least one selection from the metadata associated content to decrypt;

a network connection for establishing a secure connection with an authorization authority for decrypting the content;

a first secure container received from the computer readable medium containing the decrypting key for decrypting at least part of the previously encrypted content as permitted;

a tamper resistant environment for creating a second secure container using the encrypting key from a clearinghouse, wherein the second secure container has an encrypting key therein from the first end user system; wherein the second secure container is subsequently transferred over the network connection to the the clearinghouse for authentication of permission to decrypt the content;

a third secured container received from the clearinghouse, wherein the third secured container is encrypted using the encrypting key of the first end user system containing the decrypting key for decrypting at least part of the previously encrypted content stored on the computer readable medium as permitted; and

a fourth secured container created in the tamper resistant environment for distribution to a second end user system for playing the content which has been reencrypted with a new encrypting key associated with the first end user system.